(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－134106
（P2003－134106A）
(43)公開日　平成15年５月９日(2003.5.9)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　9/16		Ｈ０４Ｌ　9/00	６４３	５Ｊ１０４

審査請求　未請求　請求項の数５　ＯＬ　（全 ９ 頁）

(21)出願番号　特願2001－323682(P2001－323682)

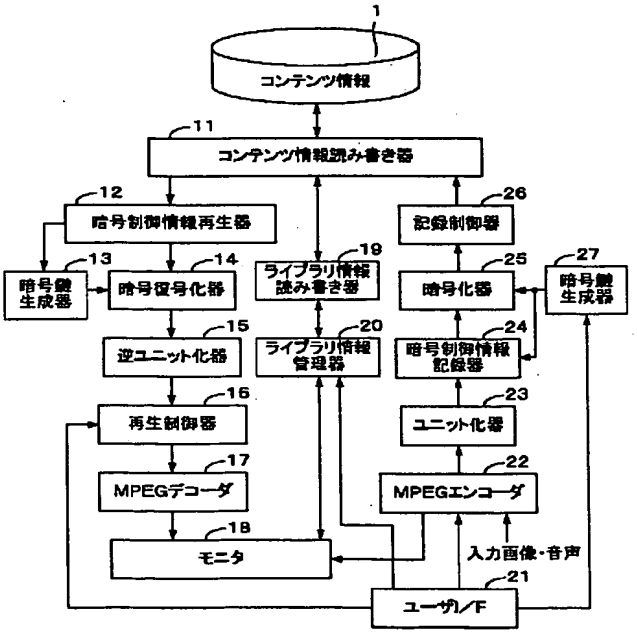
(22)出願日　平成13年10月22日(2001.10.22)

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地
(72)発明者　菅原　隆幸
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内
(72)発明者　猪羽　渉
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内
(74)代理人　100105119
弁理士　新井　孝治

最終頁に続く

(54)【発明の名称】　暗号化方法、復号化方法及び装置、並びに情報記録媒体

(57)【要約】
【課題】　従来に比べてよりセキュリティを向上させることができる暗号化方法等を提供する。
【解決手段】　暗号鍵生成器２７により、複数の情報を使用して暗号鍵が生成される。入力情報をユニット化器２３によりユニット化し、暗号制御情報記録器２４により、暗号鍵のもとになる複数の情報を特定する暗号制御情報が付加され、暗号化器２５により暗号化される。ユニット化された暗号文情報を復号化するときは、ユニットごとに保持されている暗号制御情報を用いて、そのユニットの暗号鍵のもとになる情報が特定され、そのユニットの暗号鍵のもとになる情報から暗号鍵が生成され、その暗号鍵を用いて復号化が行われる。



【特許請求の範囲】

【請求項１】 複数の情報を使用して作成した暗号鍵を用いて平文情報を暗号化し、暗号文情報を生成する暗号化方法であって、前記暗号文情報を所定の単位ごとにユニット化し、ユニットごとに、暗号鍵のもとになる前記複数の情報を特定する暗号制御情報を持たせることを特徴とする暗号化方法。

【請求項２】 所定の単位ごとにユニット化された暗号文情報を平文情報に復号化する復号化方法であって、ユニット化された暗号文情報のユニットごとに保持されている、暗号鍵のもとになる複数の情報を特定する暗号制御情報を用いて、そのユニットの暗号鍵のもとになる情報を特定し、そのユニットの暗号鍵のもとになる情報から暗号鍵を作成し、前記暗号文情報を平文情報に復号化することを特徴とする復号化方法。

【請求項３】 複数の情報を使用して生成した暗号鍵を用いて平文情報を暗号化し、暗号文情報を生成する暗号化装置であって、前記暗号文情報を所定の単位ごとにユニット化し、ユニットごとに、暗号鍵のもとになる前記複数の情報を特定する暗号制御情報を持たせることを特徴とする暗号化装置。

【請求項４】 所定の単位ごとにユニット化された暗号文情報を平文情報に復号化する復号化装置であって、ユニット化された暗号文情報のユニットごとに保持されている、暗号鍵のもとになる複数の情報を特定する暗号制御情報を用いて、そのユニットの暗号鍵のもとになる情報を特定し、そのユニットの暗号鍵のもとになる情報から暗号鍵を作成する暗号鍵作成手段と、該暗号鍵作成手段によって作成された暗号鍵を用いて、前記暗号文情報を平文情報に復号化する復号化手段とを備えることを特徴とする復号化装置。

【請求項５】 所定の単位ごとにユニット化された暗号文情報が記録され、ユニットごとに、暗号鍵の生成に必要な複数の情報を特定する暗号制御情報が記録されていることを特徴とする情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化方法及び装置、復号化方法及び装置、並びに情報記録媒体に関し、特に複数の情報を使用して作成した暗号鍵を用いて暗号化を行う暗号化方法及び装置、その暗号化方法に対応した復号化方法及び装置、並びにその暗号化方法により暗号化された情報が記録された情報記録媒体に関する。

【０００２】

【従来の技術】暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのディジタルデータを配信する有用な方法として、特開平１０－２６９２８９号公報に示されたディジタルコンテンツ配布管理方法、及びディジタルコンテンツ再生方法が知られている。この方法では、ディジタルコンテンツの配布側では、ディジタルコンテンツを暗号化及び圧縮して加工し、この加工したディジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信し、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用料金を、権利者に対して分配するようにしている。一方ディジタルコンテンツの再生側では、その加工されたディジタルコンテンツをコンテンツ鍵にて復号化すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツの使用情報を配布側に送信する。これにより、記録されたコンテンツを持ち運びできるようにしている。

【０００３】また、特開平１０－２８３２６８号公報には、情報記録媒体に、暗号化されている暗号化情報と、この暗号化情報をもとの情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるものにおいて、上記暗号化鍵情報に、非暗号化された状態で、上記暗号化情報を復号化する際の条件情報が追加記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報を含めることにより、ユーザ側で暗号化された情報をそのままＨＤＤや光ディスクにコピーし、不正使用することを防止している。

【０００４】また特開平７－１４０８９６号公報には、アプリケーションプログラムが使用するメモリ上のデータ領域とディスクバッファとの間でデータのやり取りを行なうことができる最も小さなデータサイズの平文ユニットに、平文ファイルを分割し、この平文ユニットを、ユーザ鍵でそれぞれ別々に暗号化し、暗号文ブロックを生成し、その後、生成されたｎ個の暗号文ユニットを連結して、暗号文ファイルを得る方法が開示されている。この方法によれば、アプリケーションプログラムが、ファイルに対して上書き等の部分的操作が可能な最も小さなデータサイズ毎に、平文ファイルを暗号化されるので、アプリケーションプログラムでどのような操作が行なわれようとも、いつでも元の平文ファイルに正しく復元することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、上記の特開平１０－２６９２８９号公報や特開平１０－２８３２６８号公報に示された従来の手法では、再生に制限を加えて不正使用を防止しているが、その制限情報は容易に変更することが可能であり、不正な条件で再生することを防止できないおそれがあった。

【０００６】また、特開平７－１４０８９６号公報に示された方法では、暗号化を所定のユニットに分解して行い、あとから部分的編集などが可能となるが、よりセキュリティを向上する上で改善の余地があった。本発明は上述した点に着目してなされたものであり、従来に比べてよりセキュリティを向上させることができる暗号化方法及び装置、並びに対応する復号化方法及び装置を提供することを目的とする。

【０００７】
【課題を解決するための手段】上記目的を達成するため請求項１に記載の発明は、複数の情報を使用して作成した暗号鍵を用いて平文情報を暗号化し、暗号文情報を生成する暗号化方法であって、前記暗号文情報を所定の単位ごとにユニット化し、ユニットごとに、暗号鍵のもとになる前記複数の情報を特定する暗号制御情報を持たせることを特徴とする。
【０００８】請求項２に記載の発明は、所定の単位ごとにユニット化された暗号文情報を平文情報に復号化する復号化方法であって、ユニット化された暗号文情報のユニットごとに保持されている、暗号鍵のもとになる複数の情報を特定する暗号制御情報を用いて、そのユニットの暗号鍵のもとになる情報を特定し、そのユニットの暗号鍵のもとになる情報から暗号鍵を作成し、前記暗号文情報を平文情報に復号化することを特徴とする。
【０００９】請求項３に記載の発明は、複数の情報を使用して生成した暗号鍵を用いて平文情報を暗号化し、暗号文情報を生成する暗号化装置であって、前記暗号文情報を所定の単位ごとにユニット化し、ユニットごとに、暗号鍵のもとになる前記複数の情報を特定する暗号制御情報を持たせることを特徴とする。
【００１０】請求項４に記載の発明は、所定の単位ごとにユニット化された暗号文情報を平文情報に復号化する復号化装置であって、ユニット化された暗号文情報のユニットごとに保持されている、暗号鍵のもとになる複数の情報を特定する暗号制御情報を用いて、そのユニットの暗号鍵のもとになる情報を特定し、そのユニットの暗号鍵のもとになる情報から暗号鍵を作成する暗号鍵作成手段と、該暗号鍵作成手段によって作成された暗号鍵を用いて、前記暗号文情報を平文情報に復号化する復号化手段とを備えることを特徴とする。
【００１１】請求項５に記載の発明は、所定の単位ごとにユニット化された暗号文情報が記録され、ユニットごとに、暗号鍵の生成に必要な複数の情報を特定する暗号制御情報が記録されていることを特徴とする情報記録媒体を提供する。
【００１２】
【発明の実施の形態】以下本発明の実施の形態を図面を参照して説明する。図１は本発明の一実施形態にかかる情報記録装置の構成を示すブロック図である。この装置は、アナログ入力画像信号及び音声信号をＭＰＥＧ（Motion Picture Expert Group）に準拠したディジタル信号に変換するＭＰＥＧエンコーダ２２と、ＭＰＥＧエンコーダ２２から出力されるディジタル信号をユニット化するユニット化器２３と、ユニット化されたディジタル情報に暗号制御情報を付加する暗号制御情報記録器２４と、暗号化用の暗号鍵を生成する暗号鍵生成器２７と、暗号鍵生成器２７が生成した暗号化鍵を用いて、暗号制御情報記録器２４から入力される情報の暗号化を行う暗号化器２５と、記録時の制御を行う記録制御器２６と、ユーザによる操作が入力されるユーザインターフェース２１と、記録時にプログラムのタイトル、記録開始日時などのライブラリ情報を所定の構造にフォーマットするライブラリ情報管理器２０と、ライブラリ情報の読み書きを行うライブラリ情報読み書き器１９と、記録媒体１へのコンテンツ情報の書き込み及び書き込まれたコンテンツ情報の読み出しを行うコンテンツ情報読み書き器１１と、読み出された情報から暗号制御情報などを抽出する暗号制御情報再生器１２と、復号用の暗号鍵を生成する暗号鍵生成器１３と、暗号鍵生成器１３が生成した暗号鍵を用いて、読み出された情報の復号化を行う暗号復号化器１４と、ユニット化されたデータを元に戻す逆ユニット化器１５と、再生時に、コンテンツ情報読み書き器１１の制御を行う再生制御器１６と、再生されたディジタル信号をアナログ画像信号及びアナログ音声信号に変換し、モニタ１８に出力するＭＰＥＧデコーダ１７とを備えている。
【００１３】次に、図１に示す装置の再生時の動作の概略を説明をする。ユーザインターフェース２１から所定のプログラムの詳細な情報を見るという指示が入ると図示せぬ制御用ＣＰＵは、コンテンツ情報読み書き器１１により、そのコンテンツの属性や説明を構造化して記録したライブラリ情報を記録媒体１から読み取る。そのライブラリ情報は図２に示すようにSIDE. ifoというファイルネームで、図３及び図４に示すような構造で記述されている。この構造の詳細はあとで説明する。このライブラリ情報には、プログラム単位の情報、及びそのプログラムを所定の時間区間ごと区切った単位（インデックス）ごとの情報が記録されている。それぞれには少なくともそのデータに対応するコンテンツ説明の情報が記述されている。ライブラリ情報管理器２０はそのライブラリ情報を解析して、あらかじめ決められたユーザにわかりやすいプログラム情報表示フォーマットに、ライブラリ情報画面をはめ込み、レイアウトしてモニタ１８へ画像データを伝送する。
【００１４】ユーザはモニタ１８によって、プログラムの詳細情報を得たら、ユーザインタフェース２１にて見たいプログラムを決定し、見たいプログラムのナンバをリモコンなどで入力して再生開始のボタンを押す。制御用ＣＰＵは再生開始のボタンが押されたら、再生開始信号を制御信号として再生制御器１６へ伝送する。再生制御器１６はコンテンツ情報読み書き器１１へ、再生開始の信号を伝送する。コンテンツ情報読み書き器１１は、プログラムに対応するオーディオやビデオの情報を記録媒体１から読み取り、暗号制御情報再生器１２に伝送する。暗号制御情報再生器１２は、後述する図６などに示すユニットリセット識別子と、鍵のもとの情報を特定する暗号制御情報を検出して暗号鍵生成器１３に伝送する。暗号鍵生成器１３では、暗号鍵のもとになる情報を

特定し、それをもとに暗号鍵を生成し、生成した暗号鍵を暗号復号化器１４に伝送する。暗号復号化器１４では入力された暗号鍵と、暗号化コンテンツ情報をもとに、コンテンツ情報の復号を行い、再生制御器１６を介してＭＰＥＧデコーダ１７に伝送する。オーディオやビデオの情報データは後述する図５に示す構造で記録媒体１上に記録されている。ＭＰＥＧデコーダ１７によって復号された音声や画像の信号は、所定の表示フォーマットに変換され、モニタ１８へ伝送される。モニタ１８ではそのプログラムの音声の出力や画像の表示を行う。一方、ＭＰＥＧデコーダ１７から出力される信号については、再生制御器１６により、現在再生中の画像のプログラム開始からのフレーム数が管理され、再生制御器１６は終了点を観測したら、再生を終了する制御信号をコンテンツ情報読み書き器１１へ伝送し、データ読み取りを終了する。

【００１５】次に、図１に示す装置の記録時の動作の概略を説明する。ユーザは、ユーザインタフェース２１に例えば放送からの入力画像を記録するという指示を記録開始ボタンを押すことで行う。記録開始ボタンが押されたら、図示せぬ制御用ＣＰＵは制御信号を記録制御器２６に伝送する。一方、ユーザインターフェース２１から、記録されたコンテンツプログラムのタイトルなどの情報が入力され、その情報はライブラリ情報管理器２０に伝送される。ライブラリ情報管理器２０は、プログラムのタイトルなどの情報と、記録開始日時の情報などを、後述する表１、２、及び３の構造にフォーマットし、該フォーマットした情報をライブラリ情報読み書き器１９に伝送する。ライブラリ情報読み書き器１９は、これらの情報を後述する図２、図３、及び図４の構造で記録媒体１上に記録する。

【００１６】一方、入力信号は、記録制御器２６からの記録開始信号を受けてＭＰＥＧエンコーダ２２で符号化され、ユニット化器２３へ伝送される。ユニット化器２３では図５に示すようにＭＰＥＧのトランスポートストリームパケットを所定の数ごとにユニット化してその先頭パケットの頭にＴＳユニットヘッダ領域を確保し、そこに図６に示すような暗号鍵のもとになる情報を特定する暗号制御情報を記録して、暗号化器２５に伝送する。

【００１７】ユーザは、ユーザーインタフェース２１に例えばコンテンツのセキュリティのレベルを設定する。図示せぬ制御用ＣＰＵは、その情報を暗号制御情報として、暗号鍵生成器２７へ伝送する。暗号鍵生成器２７では、暗号制御情報をもとに、後述する方法にて暗号鍵のもとになる情報を特定し、暗号鍵を生成する。この暗号鍵は暗号化器２５に伝送される。同時に暗号制御情報は暗号制御情報記録器２４へ伝送される。暗号化器２５では暗号鍵生成期２７から入力される暗号鍵を用いてＴＳユニットヘッダ以外の部分を暗号化し、記録制御器２６に伝送する。記録制御器２６では、書き込むデータが所定の単位分メモリに格納されたら、図示せぬ制御用ＣＰＵの指示に従って、記録情報をコンテンツ情報書き込み器１１へ伝送し、コンテンツ情報読み書き器１１ではコンテンツの暗号化された圧縮データを図５に示す構造で記録媒体１に記録する。

【００１８】次に、記録媒体１に記録するサイド情報（ライブラリ情報）のフォーマットについて図２，図３，及び図４と、表１、表２、及び表３とを用いて説明する。記録媒体１には、図２に示すように、ＲＯＯＴの下にTAPE_LIBという名前のフォルダが作成され、その下に複数のプログラムに関するSIDE0.ifoからSIDEn.ifoというファイルネームでサイド情報が記録される。

【００１９】SIDEj.ifo(j=1～n)のフォーマットは、図３に示すように、階層構造をもっている。一番上位にTOTAL_MANAGER_IFOが定義され、そのなかにはGENERAL_IFOとCNTNT_IFOがある。GENERAL_IFOは、この情報群全体に関するパラメータが記述される。詳細は表１に示したようなシンタックス構造になっている。

【表１】

シンタックス名	ビット数
System ID	8
Version	8
Character Set	4
Num of CNTNT_IFO	8
Start Adrs of CNTNT_IFO	32

【００２０】表１において、System_IDはこのフォーマットでかかれた情報体であることを示すＩＤである。Versionはバージョンナンバーを記述する。Character Setは後述するプログラムのテキストインフォメーションを記述しているテキストコードを記述するものである。Num of CNTNT_IFOは後述するPR_IFOの数である。StartAdrs of CNTNT_IFOはPR_IFO_0の先頭アドレスを記述するものである。

【００２１】次にCNTNT_IFO（図３）は、中身は複数のプログラムごとの情報としてPR_IFO_0からPR_IFO_nまでが記述されている。詳細は表２のようになっている。

【表２】

シンタックス名	ビット数
End Adrs of PR_IFO	32
PR nember	8
Playback Time	32
Num of INDEX	8
Rec Date	32
Rec Time	24
PR text information size	8
PR text information	Nバイト
Content nibble 1	8
Content nibble 2	8
V_ATR	32
A_ATR	32

表２において、End Adrs of PR_IFOはPR_1FOの終了アドレスである。PR numberは自分自身のプログラムナンバである。Playback Timeはそのプログラムの再生時間である。Num of INDEXはそのプログラム中をさらにいくつかのシーンに分けたもの（INDEX）の数である。Rec Dateはそのプログラムを記録した日付、Rec Timeは時刻である。PR text information sizeは後に続くプログラムに簡単な説明をつけるときのテキストインフォメーションのバイト数である。PR text informationはテキストインフォメーション情報である。Content nibbleはプログラムのジャンル情報である。V_ATRはビデオの画素サイズやビットレート、圧縮パラメータ関連の情報である。A_ATRはオーディオに関するビットレート、チャンネル数などの情報である。

【００２２】またこの下の階層に、プログラムの一部をインデックスとして登録できる構造INDEX_IFOがある。この構造のフォーマットは図４に示すようになっている。INDEX_IFOのシンタックスは表３のようになっている。

【表３】

シンタックス名	ビット数
End Adrs of INDEX_IFO	32
INDEX number	8
Playback Time	16
Start frame of INDEX	32
End frame of INDEX	32

表３のおいて、End Adrs of INDEX_IFOはINDEX_IFOの終了アドレスである。INDEX numberはプログラム内のINDEXの通しナンバである。Playback TimeはINDEXの再生時間である。Start frame of INDEXはINDEXのスタートフレームナンバである。End frame of INDEXはINDEXのエンドフレームナンバーである。

【００２３】次に、本実施形態における暗号鍵生成方法と、暗号鍵のもとの情報を特定する暗号制御情報について説明する。先に説明したＴＳユニットヘッダには図６に示すようにユニットリセット識別子と、暗号鍵のもとの情報を特定する暗号制御情報が記録される。ユニットリセット識別子は、２ビットで暗号化されているかどうかを示すビットと、後述する暗号鍵の初期値のリセットをするかどうかを指示するビットとを有する。暗号鍵のもとの情報を特定する暗号制御情報は、８ビットを割り当てて、それぞれが暗号鍵のもとになる情報を使用しているか（１）、していないか（０）を指示するビットとして記録される。暗号鍵のもとになる情報としては、例えば、プログラムナンバや、国、地域、空間を定義した領域に関する情報、個人の識別ＩＤに関する情報、複数人のグループを識別する識別ＩＤに関する情報、レーティングに関する情報、機器メーカの識別ＩＤに関する情報、コンテンツプロバイダの識別ＩＤに関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有ＩＤに関する情報、接続機器の固有ＩＤに関する情報、コンテンツの記録されたメディアの固有ＩＤに関する情報、コンテンツを識別するＩＤに関する情報、課金に関する情報などを使用する。これらのうち、実際に使用する暗号鍵のもと（シード）をここでは８個選択できるようにする。それらは図７に示すようにシード選択器によって、１のビットが立っているところに対応するシードを選択し、それぞれをハッシュ関数（文字列に数値を対応させる関数）に入力することで、所定のビット数の暗号鍵を計算する。ここで使用する暗号方式は、公開されているどんな暗号方式でも暗号鍵を用いる方式であればなんであっても良い。例えばＤＥＳ（Data Encryption Standard）方式であれば５６ビットの暗号鍵を出力するようにハッシュ関数を設計すればよい。

【００２４】また、図８に示すように、予め用いるシードのグループを設定しておいて、そのグループを例えば４つ記述できるようにして４ビットで暗号鍵のもとの情報を特定する暗号制御情報を構成しても良い。この場合、暗号鍵のもとの情報を特定する暗号制御情報のビット長を短くすることができるので、データ量削減の効果がある。また、図９に示すように上記４つのグループに番号を０から３まで対応付けして、そのグループを識別する２ビットの識別子を記述するようにしてもよい。この場合も同様に、暗号鍵のもとの情報を特定する暗号制御情報のビット長を短くすることができるので、データ量削減の効果がある。

【００２５】また、暗号制御情報は、暗号鍵のもとを特定するだけでなく、暗号初期値情報を含む暗号化に関するパラメータ情報で有っても良い。例えばＤＥＳには暗号のブロック単位の連鎖を行うモード（ＣＢＣモードなど）があり、そのために連鎖の一番最初の初期値を設定

することができる。初期値は所定の時間で有効にすることができるようにユニットリセット識別子のなかにリセットをするかどうかを指示するビットを設定できる。この初期値も工夫次第で暗号システムのセキュリティを向上する手段として使用できる。本実施形態の手法を利用すれば、例えば初期に情報を複数もっていて、そのうちどれを用いて初期値を構成するかを、暗号制御情報ビットで示すことができる。例えば図８に示すように、暗号制御情報に、８ビットを割り当てて、それぞれがその初期値情報を使用しているか（１）、していないか（０）を指示するビットとして記録する。初期値情報としても前記した、例えば、プログラムナンバや、国、地域、空間を定義したリージョンに関する情報、個人の識別ＩＤに関する情報、複数人のグループを識別する識別ＩＤに関する情報、レーティングに関する情報、機器メーカの識別ＩＤに関する情報、コンテンツプロバイダの識別ＩＤに関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有ＩＤに関する情報、接続機器の固有ＩＤに関する情報、コンテンツの記録されたメディアの固有ＩＤに関する情報、コンテンツを識別するＩＤに関する情報、課金に関する情報などを使用する。これらのうち、実際に使用する初期値情報をここでは８個選択できるようにする。それらは図１１に示すように初期値選択器によって、１のビットが立っているところに対応する初期値を選択し、それぞれをＸＯＲ関数（排他的論理和演算を行う関数）に入力することで、所定のビット数の初期値を計算する。この暗号方式は、公開されているどんな暗号方式でも初期値を用いる方式であればなんであっても良い。例えばＤＥＳ方式のＣＢＣモードであれば６４ビットのブロック初期値を出力するようにビット長の調整とともにＸＯＲ関数を設計すればよい。

【００２６】また、図１２に示すように、予め用いる初期値のグループを設定しておいて、そのグループを例えば４つ記述できるようにして４ビットで初期値情報を特定する暗号制御情報を構成しても良い。この場合、初期値情報を特定する暗号制御情報のビット長を短くすることができるので、データ量削減の効果がある。また、図１３に示すように上記４つのグループに番号を０から３まで対応付けして、そのグループを識別する２ビットの識別子を記述するようにしてもよい。この場合も同様に、初期値情報を特定する暗号制御情報のビット長を短くすることができるので、データ量削減の効果がある。

【００２７】なお、上述した実施形態では、本発明を情報記録再生装置に適用した例を示したが、図１４に示すような情報通信装置に適用することもできる。図１４に示す装置は、図１のコンテンツ情報読み書き器１１を、コンテンツ情報ＭＵＸ／ＤＥＭＵＸ器３３に置き換え、コンテンツ情報を、送信／受信制御器３２及びアンテナ３１を介して送受信するようにしたものである。これらの構成要素以外は、図１の装置と同一である。

【００２８】この装置では、コンテンツ情報とライブラリ情報が、コンテンツ情報ＭＵＸ／ＤＥＭＵＸ器３３により多重化されて送信されるとともに、多重化されて送信されたコンテンツ情報とライブラリ情報を受信して、コンテンツ情報ＭＵＸ／ＤＥＭＵＸ器３３により分離化が行われる。その際、送信／受信制御器３２により、コンテンツ情報の送受信の制御が行われる。

【００２９】また、本発明の信号データを記録した記録媒体１は、暗号化制御情報を用いて媒体のデータを再生できるという媒体特有の効果があり、この暗号化制御情報を用いて暗号化セキュリティを向上させることができ、高セキュリティを有するプリレコーデッド記録媒体などのビジネスを実現できるなどコンテンツ情報配送、配信システムを好適に実現することができる。

【００３０】また、記録媒体１は、例えば磁気ディスク、磁気テープ、光ディスクといったデータを記録できる媒体という、狭義な媒体というものだけでなく、信号データを伝送するための電磁波、光などを含む。また、記録媒体に記録されている情報は、記録されていない状態での、電子ファイルなどのデータ自身を含むものとする。

【００３１】

【発明の効果】以上詳述したように請求項１または３に記載の発明によれば、暗号文情報が所定の単位ごとにユニット化され、ユニットごとに、暗号鍵のもとになる複数の情報を特定する暗号制御情報が保持されるので、部分的編集などが可能な構成をとりながら、ユニットごとに異なる暗号制御情報を保持させることにより、暗号鍵を容易に変更することができるようになり、セキュリティの向上を図ることできる。

【００３２】請求項２または４に記載の発明によれば、ユニット化された暗号文情報のユニットごとに記録されている、暗号鍵のもとになる複数の情報を特定する暗号制御情報を用いて、そのユニットの暗号鍵のもとになる情報が特定され、そのユニットの暗号鍵のもとになる情報から暗号鍵が作成され、暗号化された暗号文情報が平文情報に復号化されるので、ユニットごとに暗号鍵が変更されても容易に対応することができ、正しい復号化を行うことできる。

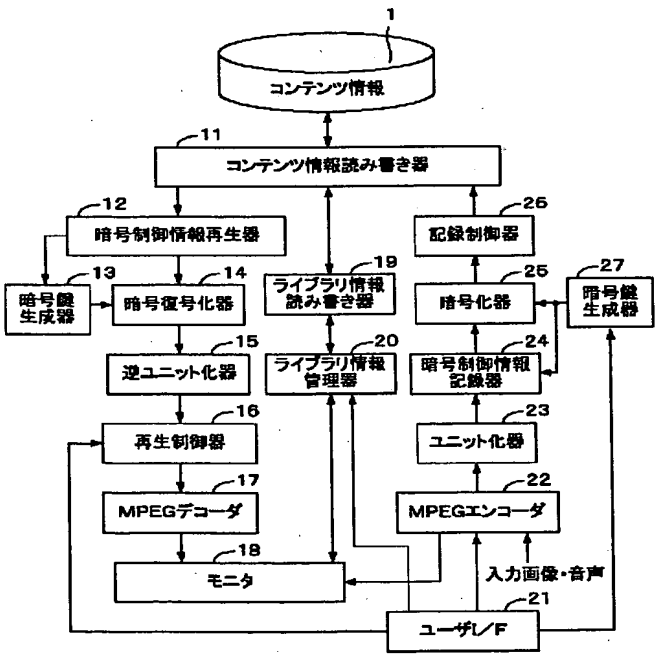
【００３３】請求項５に記載の発明によれば、所定の単位ごとにユニット化された暗号文情報が記録され、ユニットごとに、暗号鍵の生成に必要な複数の情報を特定する暗号制御情報が記録されている情報記録媒体が提供されるので、暗号化制御情報をユニットごとに異なるものとすることにより、不正なコピーがおこなわれても再生が困難なものとなり、セキュリティの向上を図ることができる。

【図面の簡単な説明】

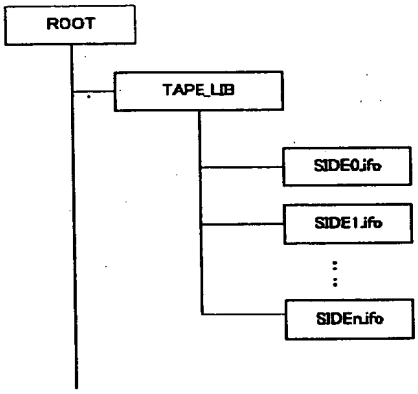
【図１】本発明の一実施形態にかかる情報記録再生装置

の構成を示すブロック図である。
【図２】記録媒体にライブラリ情報を記録する場合のファイル構成を示す図である。
【図３】図２に示すファイル内の構造を示す図である。
【図４】図３に示す構造の下位構造を示す図である。
【図５】記録媒体上のデータフォーマットを示す図である。
【図６】暗号制御情報のフォーマット例を示す図である。
【図７】暗号制御情報から暗号鍵を生成する手順を説明するための図である。
【図８】暗号制御情報のフォーマット例を示す図である。
【図９】暗号制御情報のフォーマット例を示す図である。
【図１０】暗号制御情報のフォーマット例を示す図である。
【図１１】暗号制御情報から初期値を生成する手順を説明するための図である。
【図１２】暗号制御情報のフォーマット例を示す図である。
【図１３】暗号制御情報のフォーマット例を示す図である。
【図１４】本発明の他の実施形態にかかる情報送受信装置の構成を示すブロック図である。
【符号の説明】
１２　暗号制御情報再生器（暗号鍵作成手段）
１３　暗号鍵生成器（暗号鍵作成手段）
１４　暗号復号器（復号化手段）
１５　逆ユニット化器
２３　ユニット化器
２４　暗号制御情報記録器
２５　暗号化器
２７　暗号鍵生成器

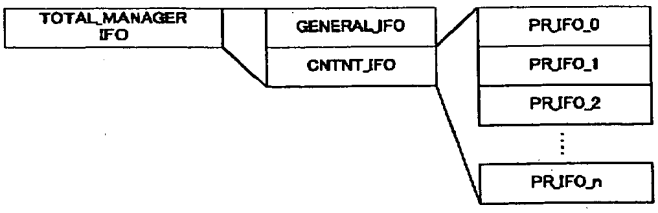
【図１】



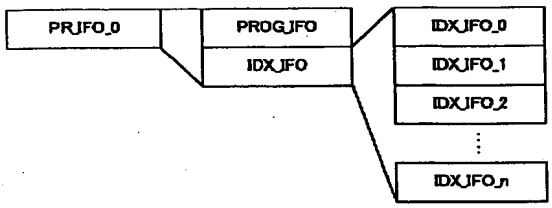
【図２】



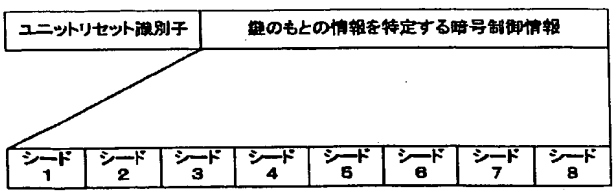
【図３】



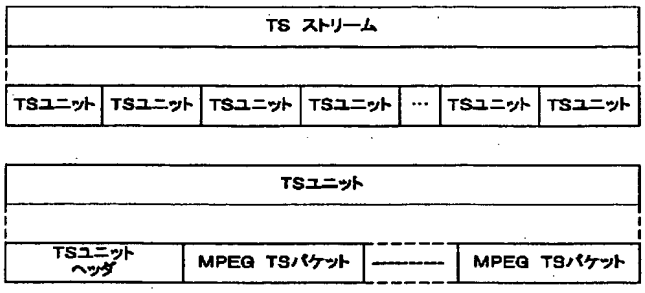
【図４】



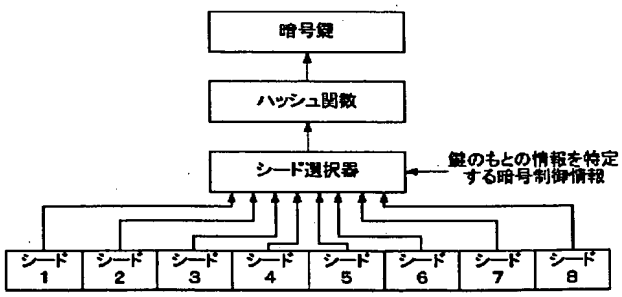
【図６】



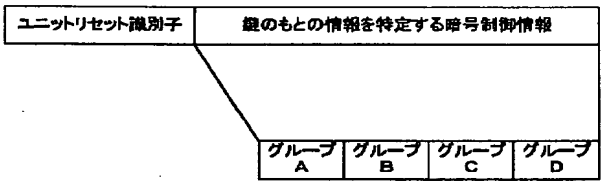
【図５】



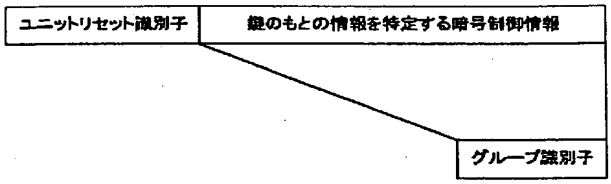
【図７】



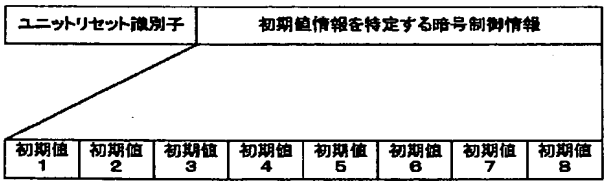
【図８】



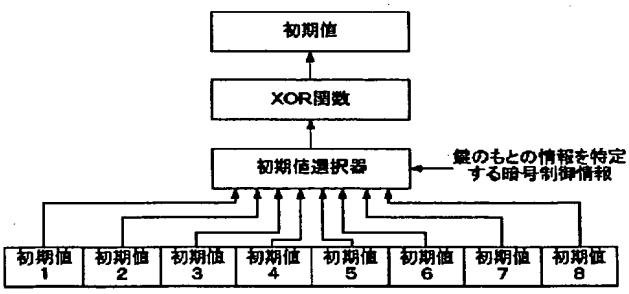
【図９】



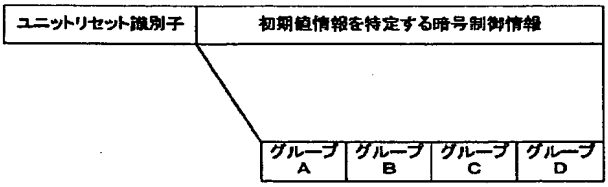
【図１０】



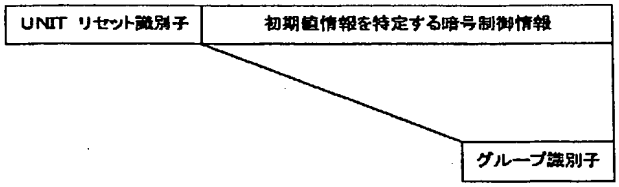
【図１１】



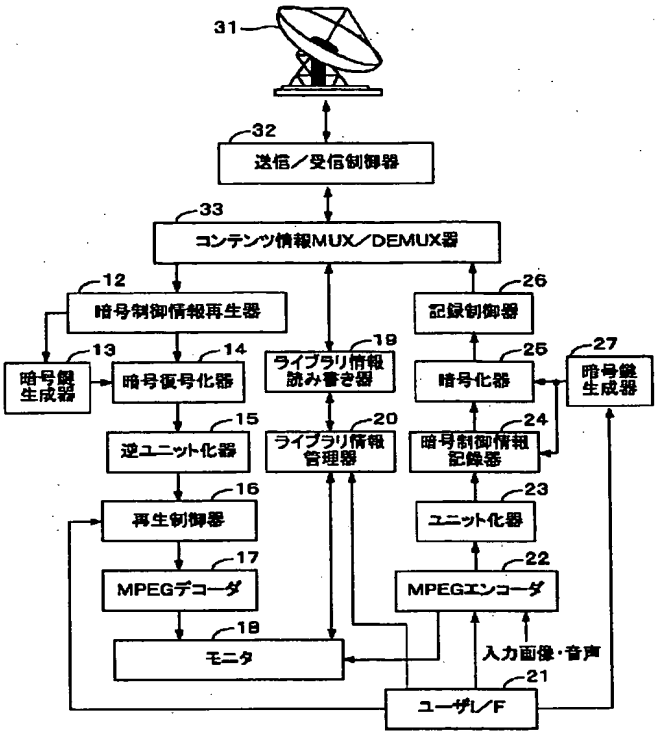
【図１２】



【図１３】



【図１４】



フロントページの続き

(72)発明者　日暮　誠司
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

(72)発明者　黒岩　俊夫
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

(72)発明者　上田　健二朗
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

Ｆターム(参考)　5J104 AA01 AA35 NA02 PA14